SOUTHERN ROOFING & RENOVATIONS

COMPUTER USER AGREEMENT

This agreement applies to all SNR Global, LLC employees, volunteers, staffing agency personnel, independent contractors, vendors and anyone else granted access to SRNR computing systems. The computer user agreement encompasses the use of all SRNR owned computers, mobile devices, and electronic communication systems such as email, voicemail and the Internet, as well as the use of personal computing devices to conduct SRNR business. For the purposes of this agreement, the terms "individual" and "staff" are inclusive of employees, volunteers, staffing agency personnel, independent contractors, vendors and anyone else granted access to SRNR computing systems. Violation of any portion of this policy may result in termination of employment and/or relationship with SRNR.

Login and Password Confidentiality:

- SRNR issues computer logins and passwords that allow access to organization information systems. Computer passwords are confidential and should not be revealed to anyone, except Information Technology (IT) department staff, as required.

Authorized Access and Confidentiality of Records:

- Staff are to access information on company computers only as authorized and required for their job duties. Unauthorized access, use, modification, copying or deletion of information is prohibited.
- Computer-based financial, personnel, payroll, and other data are considered as confidential as their paper-based equivalent documents. Individuals are expected to respect and maintain the confidentiality and security of these records as required by the confidentiality policy which is part of the Compliance Program. All individuals receive a copy, or have electronic access to the document, and agree to adhere to the SRNR Compliance Program.

Ownership of Information:

- All electronic information on all equipment remains the exclusive property of SRNR has the capacity to access, review, copy, modify and delete any information transmitted through or stored in the system, including email messages and visits to Internet sites.
- SRNR may conduct audits of staff use of computers and communications systems and reserves the right to access, review, copy, modify or delete all such information for any purpose and to disclose it to any party (inside or outside SRNR) it deems appropriate.
- Individuals who become aware of potential security breaches, security incidents, and inappropriate Internet use must report it to the Director of IT and Head of HR and Risk Management.

Email and Internet Use:

- Email and Internet access for SRNR staff will be granted based on job-related need and may be discontinued at any time.
- Any employee who uses Internet services, including email, that have been supplied by SRNR should be aware that computerized communications can be intercepted, and any such employee should take all proper precautions when discussing confidential information relating to SRNR

  business.
- The use of email and Internet access must be primarily for SRNR business-related activity. Limited personal use is acceptable during breaks provided its use does not degrade the SRNR public image, adversely affects network resources, or presents a security risk. Inappropriate email or Internet use may result in discipline, up to and including termination. Inappropriate use includes, but is not limited to the following activities:
    - More than incidental personal use during break time
    - Accessing or downloading pornographic, sexually explicit, or other offensive material
    - Using computers for any type of gaming, gambling, soliciting for person gain or profit, to disrupt operation of computer or network, soliciting staff to send any form of chain
    - Downloading any type of software without expressed permission from Information Services onto computer or SRNR owned mobile device, this includes games and personal apps
    - Posting indecent or inappropriate remarks which may be damaging or embarrassing to SRNR such as using SRNR controlled or personal social media accounts
    - Using non-approved SRNR instant messaging applications. SRNR's preferred instant messaging platform is Microsoft Teams.
    - Streaming Video or Audio for personal use, such as YouTube, Internet Radio, videos, etc.
    - Business or commercial activity not related to or authorized by appropriate SRNR management
    - Disclosure, inadvertent or intended, of confidential information or transmission of such information without adequate security precautions
    - Use of SRNR resources for the purpose of assisting a campaign for election to an office, except as specifically authorized by appropriate SRNR management
    - Other illegal or criminal activity

Computer / Software Use:

- SRNR issues personal computers and software to staff for use in their work. The use of computing devices presents a risk that confidential information accessible through such devices may be illegally used, accessed, or disclosed.
- The hard drive of a computer (laptop or workstation) will not be used to store confidential data.

- USB drives (thumb drives) and other portable digital media such as memory cards are prohibited without expressed permission from Information Technology. Information Technology will provide alternative solutions for users requiring remote access to files.
- The use of Cloud-based file sharing services (e.g. Dropbox, Google Drive, iCloud, etc.) is prohibited without expressed permission from Information Technology. The one exception is Microsoft's OneDrive which is licensed and configured on a per user basis as part of SRNR's Office365 subscription.
- Individuals may not install software on the computers provided by SRNR except as authorized by Information Services. This includes personal software and non-approved business software.
- SRNR observes and enforces the terms of software licenses. Staff members may not use, copy, or install any of the company's software or related manuals in any manner that violates the licensing agreements of those products. Only Information Technology or an authorized agent appointed by Information Technology may install or copy software on or from the SRNR computers.

Mobile & Portable Devices:

- Mobile and portable devices include smartphones (e.g., iPhone and Android devices), notebook computers, and tablet computers (e.g., iPad and Surface devices). Staff may be provided with these devices in order to do their job. The type of device and connection method (e.g. VPN, VDI, or email configuration) will be determined on a case-by-case basis based on business need.
- Information Services will install, and support company owned devices.
- Non-company-owned devices may be connected to SRNR computers and networks only if approved in advance by the staff member's manager due to a business need and if determined by Information Technology not to be a security risk.

Servicing SRNR Supplied Computers:

- Any SRNR supplied computer (workstation or laptop) that requires service shall be serviced by Information Technology or an authorized agent appointed by Information Technology. Employees shall promptly notify Information Technology if any SRNR supplied computer or software requires service.

Relocating or Reassigning SRNR Supplied Equipment:

- Employees are prohibited from relocating or reassigning SRNR supplied computers (workstation or laptop), desktop phones, mobile devices, or cell phones. Employees shall promptly notify Information Technology if any SRNR supplied equipment needs to be physically relocated or reassigned.

AGREEMENT

I have read and understand the above requirements and agree to adhere to them. I also understand that I have no right to privacy related to my use of agency computers and that SRNR may provide information to legal and regulatory authorities if illegal, unauthorized or criminal activity is suspected.

All employees, volunteers, staffing agency personnel, independent contractors, vendors and anyone else granted access to SRNR computing systems are required to sign this agreement confirming their understanding and acceptance of this policy.

Signature: _____ Date: _____

Name: _____ Department: _____

(Please Print)

verifies the Electronic Signature of this document

SIGNATURE	
Signer Name:	Leah Raffles
User ID:	leahraffles
Date Electronically Signed:	Apr 14, 2025 03:46 PM EDT
File Name:	Computer User Agreement.docx-adpdms-3926874602593.docx
Display Name:	Computer User Agreement.docx